

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
17 November 2005 (17.11.2005)

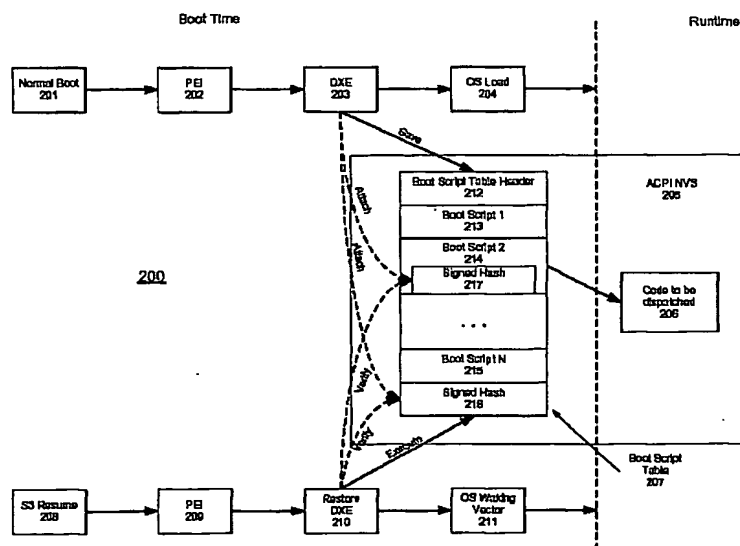
PCT

(10) International Publication Number
WO 2005/109184 A1

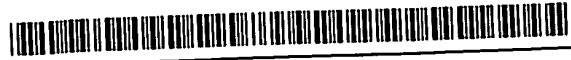
- (51) International Patent Classification⁷: **G06F 9/00**, 9/44, 11/00
- (21) International Application Number: **PCT/CN2004/000447**
- (22) International Filing Date: **8 May 2004 (08.05.2004)**
- (25) Filing Language: **English**
- (26) Publication Language: **English**
- (71) Applicant (for all designated States except US): **INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).**
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **CHEN, Lechong [CN/CN]; N31 Apt. 1003 Lane 1555, Kai Xuan Bei Road, Shanghai 200063 (CN). XING, Bin [CN/CN]; N12 Apt. 502 Nong 250 Lixi Road, Changning District, Shanghai 200050 (CN). JIN, Feng [CN/CN]; N13 Apt. 405, 30 Le Shan Road, Shanghai 200030 (CN).**
- (74) Agent: **RUNPING & PARTNERS; Suite 509, Yingu Mansion, No. 9 Beisihuanxilu, Haidian District, Beijing 100080 (CN).**
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): **AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.**
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): **ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).**

[Continued on next page]

(54) Title: **FIRMWARE INTERFACE RUNTIME ENVIRONMENT PROTECTION FIELD**



(57) Abstract: Method and apparatus for protecting a firmware runtime environment are described herein. In one embodiment, a process example is provided to retrieve a first key from a secure store of a firmware within a platform, the firmware including an initialization table for initializing the platform, and verify the initialization table using the first key retrieved from the secure store during an initialization of the platform. Other methods and apparatuses are also described.



Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.